Claim:

1. A decryption method with usage of a digital information processing device for decrypting cyphertext corresponding to plaintext and expressed by an element of a finite extension field of a prime field, wherein said element has a plurality of sub-elements, comprising:

a step for multiplying the cyphertext by a first secret key; and

a step for permuting the sequence of the sub-elements in the cyphertext in such a way that said sub-elements are separated into a part corresponding to the plaintext and noise.

2. A decryption method according to claim 1, wherein said cyphertext is obtained by substituting the plaintext for an indeterminate of a first polynomial.

3. A decryption method according to claim 1, wherein said first secret key is one of powers of a primitive root of a primitive polynomial in the finite extension field.

4. A decryption method according to claim 1, further comprising a step for multiplying said part corresponding to the plaintext by a third secret key comprising a second polinomial to a product.

5. A decryption method according to claim 1, further comprising a step for obtaining a power root of said product.

6. A decryption method for decrypting cyphertext corresponding to plaintext

and expressed by an element of a finite extension field of a prime field with usage of a digital information processing device, wherein said element has a plurality of sub-elements, comprising:

sending to said digital information processing device a computer program including a sub-program for multiplying the cyphertext by a first secret key, and a sub-program for permuting the sequence of the sub-elements in the cyphertext in such a way that said sub-elements are separated into a part corresponding to the plaintext and noise; and

making said digital information processing device decrypt the cyphertext according to said computer program.

7. A decryption method according to claim 6, wherein said cyphertext is obtained by substituting the plaintext for an indeterminate of a first polynomial.

8. A decryptor for decrypting cyphertext corresponding to plaintext and expressed by an element of a finite extension field of a prime field, wherein said element has a plurality of sub-elements, comprising:

a multiplication means for multiplying the cyphertext by a first secret key; and

a permutation means for permuting the sequence of the sub-elements in the cyphertext in such a way that said sub-elements are separated into a part corresponding to the plaintext and noise.

9. A decryptor according to claim 8, wherein said cyphertext is an evaluation of a first polynomial at the plaintext.

10. A decryptor according to claim 8, wherein said multiplication means multiplies the cyphertext by one of powers of a primitive root of a primitive polynomial in the finite extension field as the first secret key, and further comprising a means for multiplying said part corresponding to the plaintext by a third secret key comprising a second polinomial into a product and for obtaining a power root of said product.

11. A recording medium, for decrypting cyphertext corresponding to plaintext and expressed by an element of a finite extension field of a prime field comprising a plurality of sub-elements, retrievable by a digital information processing device, and for making the digital information processing device perform:

a step for multiplying the cyphertext by a first secret key; and

a step for permuting the sequence of the sub-elements in the cyphertext in such a way that said sub-elements are separated into a part corresponding to the plaintext and noise.

12. A propagating signal, for decrypting cyphertext corresponding to plaintext and expressed by an element of a finite extension field of a prime field comprising a plurality of sub-elements, and storing codes retrievable by a digital information processing device and for making said digital information processing device perform:

a step for multiplying the cyphertext by a first secret key; and

a step for permuting the sequence of the sub-elements in the cyphertext in such a way that said sub-elements are separated into a part corresponding to the plaintext and noise.